

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-254909

(43)公開日 平成10年(1998) 9月25日

(51)Int.Cl.⁶

識別記号

F I

G 0 6 F 17/30

G 0 6 F 15/40

3 2 0 B

15/00

3 3 0

15/00

3 3 0 Z

G 0 9 C 1/00

G 0 9 C 1/00

6 6 0 F

5/00

5/00

H 0 4 N 1/387

H 0 4 N 1/387

審査請求 未請求 請求項の数29 F D (全 21 頁) 最終頁に続く

(21)出願番号

特願平9-76555

(22)出願日

平成9年(1997) 3月12日

(71)出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72)発明者 斉藤 誠

東京都千代田区丸の内二丁目6番3号 三

菱商事株式会社内

(74)代理人 弁理士 南條 眞一郎

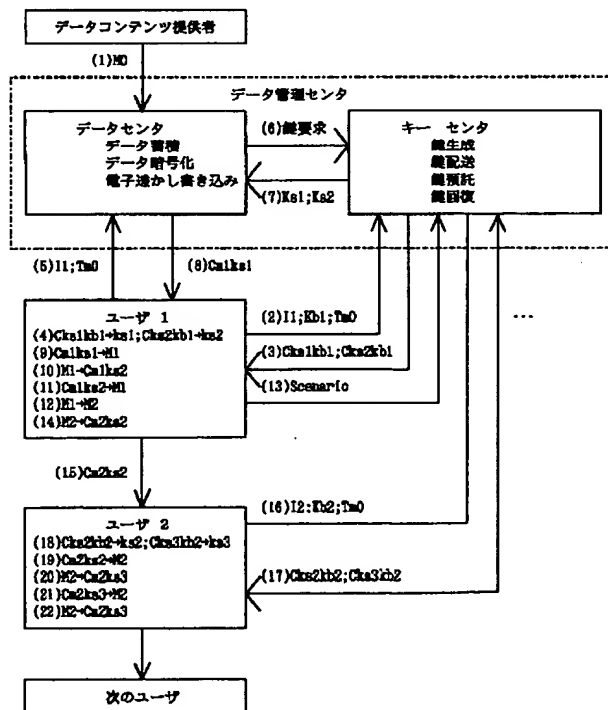
(54)【発明の名称】 データ管理システム

(57)【要約】

(修正有)

【課題】 データコンテンツの盗用や漏洩の防止。

【解決手段】 ユーザに供給されるデータコンテンツにはデータ管理センタでユーザデータが電子透かしとして埋め込まれ、データコンテンツが暗号鍵で暗号化されて供給される。暗号化データコンテンツはデータ管理センタからの暗号鍵を用いて復号して利用され、保存では別の暗号鍵を用いて暗号化される。データコンテンツを他のユーザに複写・転送するには、他のユーザのユーザデータを電子透かしを埋め込むシナリオがデータ管理センタに登録され、電子透かしが埋め込まれたデータコンテンツが別の暗号鍵で暗号化されて供給される。シナリオで他のユーザの正当性が確認されると、他のユーザに別の暗号鍵が配送され、暗号化データコンテンツは別の暗号鍵で復号して利用され、保存では別の暗号鍵で暗号化される。データコンテンツの不正な複写・転送が行われた場合には電子透かしの確認でその利用者を特定できる。



【特許請求の範囲】

【請求項1】ユーザがデータセンタのデータコンテンツを利用するデータ管理システムであって：前記データ管理システムは、

データセンタとキーセンタからデータ管理センタが構成され；第1ユーザは前記キーセンタに、データコンテンツ名を指定し、ユーザデータを提示して第1秘密鍵及び第2秘密鍵の配送を要求し；前記第1秘密鍵及び前記第2秘密鍵の配送を要求された前記キーセンタは、前記第1秘密鍵及び前記第2秘密鍵を生成し前記データコンテンツ名、前記第1ユーザデータ、前記第1秘密鍵及び前記第2秘密鍵を保管するとともに、前記第1秘密鍵及び前記第2秘密鍵を前記第1ユーザに配送し；前記第1秘密鍵及び前記第2秘密鍵を配送された前記第1ユーザは配送された前記第1秘密鍵及び前記第2秘密鍵を装置内に保存し；前記第1秘密鍵及び前記第2秘密鍵を装置内に保存した前記第1ユーザが、前記第1ユーザデータを提示し、前記データコンテンツ名を指定して前記データセンタに前記データコンテンツの配送を要求し；前記データコンテンツの配送を要求された前記データセンタが、前記第1ユーザが提示した前記第1ユーザデータ及び前記データコンテンツ名を前記キーセンタに転送して前記第1秘密鍵及び前記第2秘密鍵の転送を依頼し；前記第1ユーザデータ及び前記データコンテンツ名を転送された前記キーセンタが、前記第1秘密鍵及び前記第2秘密鍵を前記データセンタに転送し；前記第1秘密鍵及び前記第2秘密鍵を転送された前記データセンタは、前記第1ユーザデータを前記第1ユーザが要求する前記データコンテンツに電子透かしとして埋め込んで第1加工データコンテンツに加工し、前記第1加工データコンテンツを前記第1秘密鍵を用いて暗号化して第1暗号化加工データコンテンツとし、前記第1ユーザに配送するとともに前記第1加工データコンテンツの加工プロセスの第1シナリオを保管し；前記第1暗号化加工データコンテンツを配送された前記第1ユーザが、前記第1暗号化加工データコンテンツを前記第1秘密鍵を用いて復号して利用し、この時に前記第1秘密鍵が破棄され；前記第1加工データコンテンツが保存装置内に保存される際には、前記第2秘密鍵を用いて暗号化されて保存され；前記第1暗号化加工データコンテンツが再利用される際には、前記第2秘密鍵を用いて再復号されて再利用され；前記第1加工データコンテンツが再保存される際には、前記第2秘密鍵を用いて再暗号化されて保存され；前記第1ユーザが前記第1加工データコンテンツを第2ユーザに転送する時には、前記第1ユーザが第2ユーザデータを前記第1加工データコンテンツに電子透かしとして埋め込んで第2加工データコンテンツに加工し、前記第2加工データコンテンツを前記第2秘密鍵を用いて暗号化して第2暗号化加工データコンテンツとし、前記第2ユーザに転送するとともに前記第2加工デ

ータコンテンツの加工プロセスの第2シナリオを前記キーセンタに転送して登録し；前記第2暗号化加工データコンテンツを転送された前記第2ユーザは前記キーセンタに前記データコンテンツ名を指定し、前記第2ユーザデータを提示して前記第2秘密鍵及び第3秘密鍵の配送を要求し；前記第2秘密鍵及び前記第3秘密鍵の配送を要求された前記キーセンタは前記第2シナリオによって前記第2ユーザが正当なユーザであることを確認し、前記第3秘密鍵を生成し保管するとともに、前記第2秘密鍵及び前記第3秘密鍵を前記第2ユーザに配送し；前記第2秘密鍵及び前記第3秘密鍵を配送された前記第2ユーザが前記第2暗号化加工データコンテンツを前記第2秘密鍵を用いて復号して利用し、この時に前記第2秘密鍵が破棄され；第2加工データコンテンツが保存される際には、前記第3秘密鍵を用いて再暗号化されて保存され；前記第2加工データコンテンツが再利用される際には前記第3秘密鍵を用いて復号されて再利用され；前記第2加工データコンテンツが再保存される際には、前記第3秘密鍵を用いて前記第2加工データコンテンツが再暗号化されて再保存され；以後、同様な動作が繰り返される。

【請求項2】ユーザがデータセンタのデータコンテンツを利用するデータ管理システムであって：前記データ管理システムは、

データセンタとキーセンタからデータ管理センタが構成され；第1ユーザは前記キーセンタに、データコンテンツ名を指定し、ユーザデータを提示して第1秘密鍵及び第2秘密鍵の配送を要求し；前記第1秘密鍵及び前記第2秘密鍵の配送を要求された前記キーセンタは、前記第1秘密鍵及び前記第2秘密鍵を生成し前記データコンテンツ名、前記第1ユーザデータ及び前記第1秘密鍵及び前記第2秘密鍵を保管するとともに、前記第1秘密鍵及び前記第2秘密鍵を前記第1ユーザに配送し；前記第1秘密鍵及び前記第2秘密鍵を配送された前記第1ユーザは配送された前記第1秘密鍵及び前記第2秘密鍵を装置内に保存し；前記第1秘密鍵及び前記第2秘密鍵を装置内に保存した前記第1ユーザが、前記第1ユーザデータを提示し、前記データコンテンツ名を指定して前記データセンタに前記データコンテンツの配送を要求し；前記データコンテンツの配送を要求された前記データセンタが、前記第1ユーザが提示した前記第1ユーザデータ及び前記データコンテンツ名を前記キーセンタに転送して前記第1秘密鍵及び前記第2秘密鍵の転送を依頼し；前記第1ユーザデータ及び前記データコンテンツ名を転送された前記キーセンタが、前記第1秘密鍵及び前記第2秘密鍵を前記データセンタに転送し；前記第1秘密鍵及び前記第2秘密鍵を転送された前記データセンタは、前記第1ユーザデータを前記第1ユーザが要求する前記データコンテンツに電子透かしとして埋め込んで第1加工データコンテンツに加工し、前記第1加工データコンテ

3

ンツを前記第1秘密鍵を用いて暗号化して第1暗号化加工データコンテンツとし、前記第1ユーザに配送するとともに前記第1加工データコンテンツの加工プロセスの第1シナリオを保管し；前記第1暗号化加工データコンテンツを配送された前記第1ユーザが、前記第1暗号化加工データコンテンツを前記第1秘密鍵を用いて復号して利用し、この時に前記第1秘密鍵が破棄され；前記第1加工データコンテンツが保存装置内に保存される際には、前記第2秘密鍵を用いて暗号化されて保存され；前記第1暗号化加工データコンテンツが再利用される際には、前記第2秘密鍵を用いて復号されて利用され；前記第1加工データコンテンツが再保存される際には、前記第2秘密鍵を用いて再暗号化されて再保存され；前記第1ユーザが前記第1加工データコンテンツを第2ユーザに転送する時には、前記第1ユーザが第2ユーザデータを前記第1加工データコンテンツに電子透かしとして埋め込んで第2加工データコンテンツに加工し、前記第2加工データコンテンツを前記第2秘密鍵を用いて暗号化して第2暗号化加工データコンテンツとし、前記第2ユーザに転送するとともに前記第2加工データコンテンツの加工プロセスの第2シナリオを前記キーセンタに転送して登録し；前記第2シナリオを転送された前記キーセンタは、第3秘密鍵を生成し、前記第2シナリオと前記第3秘密鍵を保管するとともに前記第3秘密鍵を前記第1ユーザに配送し；前記第3秘密鍵を配送された前記第1ユーザは前記第3秘密鍵を用いて前記第2加工データコンテンツを暗号化し、暗号化第2加工データコンテンツを前記第2ユーザに転送し；前記暗号化第2加工データコンテンツを転送された前記第2ユーザは前記キーセンタに前記データコンテンツ名を指定し、第2ユーザデータを提示して前記第3秘密鍵及び第4秘密鍵の配送を要求し；前記第3秘密鍵及び第4秘密鍵の配送を要求された前記キーセンタは前記第2シナリオによって前記第2ユーザが正当なユーザであることを確認し、前記第4秘密鍵を生成し保管するとともに、前記第3秘密鍵及び前記第4秘密鍵を前記第2ユーザに配送し；前記第3秘密鍵及び前記第4秘密鍵を配送された前記第2ユーザが前記第2暗号化加工データコンテンツを前記第3秘密鍵を用いて復号して利用し、この時に前記第3秘密鍵が破棄され；前記第2加工データコンテンツが保存される際には、前記第4秘密鍵を用いて再暗号化されて保存され；前記第2加工データコンテンツが再利用される際には前記第4秘密鍵を用いて復号されて再利用され；前記第2加工データコンテンツが再保存される際には、前記第4秘密鍵を用いて前記第2加工データコンテンツが再暗号化されて再保存され；以後、同様な動作が繰り返される。

【請求項3】ユーザがデータセンタのデータコンテンツを利用するデータ管理システムであって：前記データ管理システムは、

4

データセンタとキーセンタからデータ管理センタが構成され；第1ユーザは前記データ管理センタに、データコンテンツ名を指定し、ユーザデータを提示して第1秘密鍵、第2秘密鍵及びデータコンテンツの配送を要求し；前記第1秘密鍵、前記第2秘密鍵及び前記データコンテンツの配送を要求された前記データ管理センタは、前記第1秘密鍵及び前記第2秘密鍵を生成し前記データコンテンツ名、前記第1ユーザデータ、前記第1秘密鍵及び前記第2秘密鍵を保管するとともに、前記第1ユーザデータを前記データコンテンツに電子透かしとして埋め込んで第1加工データコンテンツに加工し、前記第1加工データコンテンツを前記第1秘密鍵を用いて暗号化して第1暗号化加工データコンテンツとし、前記第1暗号化加工データコンテンツ前記第1ユーザに配送するとともに前記第1加工データコンテンツの加工プロセスの第1シナリオを保管し；前記第1秘密鍵、前記第2秘密鍵及び前記第1暗号化加工データコンテンツを配送された前記第1ユーザは配送された前記第1秘密鍵及び前記第2秘密鍵を装置内に保存するとともに前記第1秘密鍵を用いて前記第1暗号化データコンテンツを復号して利用し、この時に前記第1秘密鍵が破棄され；前記第1加工データコンテンツが保存装置内に保存される際には、前記第2秘密鍵を用いて暗号化されて保存され；前記第1暗号化加工データコンテンツが再利用される時には、前記第2秘密鍵を用いて再復号されて再利用され；前記第1加工データコンテンツが保存装置内に再保存される時には、前記第2秘密鍵を用いて再暗号化されて再保存され；前記第1ユーザが前記第1加工データコンテンツを第2ユーザに転送する時には、前記第1ユーザが第2ユーザデータコンテンツを前記第1加工データコンテンツに電子透かしとして埋め込んで第2加工データコンテンツに加工し、前記第2加工データコンテンツを前記第2秘密鍵を用いて暗号化して第2暗号化加工データコンテンツとし、前記第2ユーザに転送するとともに前記第2加工データコンテンツの加工プロセスの第2シナリオを前記データ管理センタに転送して登録し；前記第2暗号化加工データコンテンツを転送された前記第2ユーザは前記データ管理センタに前記データコンテンツ名を指定し、前記第2ユーザデータを提示して前記第2秘密鍵及び第3秘密鍵の配送を要求し；前記第2秘密鍵及び前記第3秘密鍵の配送を要求された前記データ管理センタは前記第2シナリオによって前記第2ユーザが正当なユーザであることを確認し、前記第3秘密鍵を生成し保管するとともに、前記第2秘密鍵及び前記第3秘密鍵を前記第2ユーザに配送し；前記第2秘密鍵及び前記第3秘密鍵を配送された前記第2ユーザが前記第2暗号化加工データコンテンツを前記第2秘密鍵を用いて復号して利用し、この時に前記第2秘密鍵が破棄され；前記第2加工データコンテンツが保存される際には、前記第3秘密鍵を用いて再暗号化されて保存され；前記第2加工データ

コンテンツが再利用される際には前記第 3 秘密鍵を用いて復号されて再利用され；前記第 2 加工データコンテンツが再保存される際には、前記第 3 秘密鍵を用いて前記第 2 加工データコンテンツが再暗号化されて再保存され；以後、同様な動作が繰り返される。

【請求項 4】ユーザがデータ管理センタのデータコンテンツを利用するデータ管理システムであって：前記データ管理システムでは、

データ管理プログラムがユーザデータ及び秘密鍵をスロットに格納するオブジェクトプログラムとして構成されており；第 1 ユーザが第 1 秘密鍵を用いて暗号化された暗号化データコンテンツを入手し；前記暗号化データコンテンツを入手した第 1 ユーザは、前記第 1 秘密鍵がスロットに格納された前記データ管理プログラムオブジェクトを前記データ管理センタから入手して前記第 1 ユーザデータをデータ管理プログラムオブジェクトのスロットに格納し；前記第 1 ユーザデータがデータ管理プログラムオブジェクトに格納済みであることが前記データ管理プログラムにより確認されると前記第 1 ユーザデータに基づく電子透かしパターンを生成され；前記第 1 秘密鍵を用いて前記暗号化データコンテンツが復号され、復号された前記データコンテンツには直ちに前記電子透かしを埋め込まれて第 1 加工データコンテンツとされ；データ管理プログラムにより第 2 秘密鍵が生成されて保存され、この時に前記第 1 秘密鍵が廃棄され；その後前記第 1 加工データコンテンツが利用され；前記第 1 加工データコンテンツが保存される際には、初めに前記第 2 秘密鍵を用いて前記第 1 加工データコンテンツが再暗号化されて第 1 暗号化加工データコンテンツとされ；前記第 1 加工データコンテンツが前記第 1 暗号化加工データコンテンツとされているか否かが確認されると前記第 1 暗号化加工データコンテンツが保存され；前記第 1 ユーザが前記第 1 暗号化データコンテンツを再利用する場合には、前記第 1 暗号化データコンテンツを前記第 2 秘密鍵を用いて復号して前記第 1 データコンテンツを利用し；前記第 1 ユーザが再利用した前記第 1 データコンテンツを保存する際には、前記第 2 秘密鍵を用いて前記第 1 データコンテンツが再暗号化されて前記第 1 暗号化データコンテンツが保存され；前記第 1 ユーザが前記第 1 暗号化データコンテンツを第 2 ユーザに対して複写・転送する際には前記第 1 暗号化データコンテンツが複写・転送され；以後、同様な動作が繰り返される。

【請求項 5】前記データセンタと前記キーセンタが別個の組織である請求項 1 又は請求項 2 記載のデータ管理システム。

【請求項 6】前記データセンタと前記キーセンタが前記データ管理センタに単一の組織として含まれている請求項 1 又は請求項 2 記載のデータ管理システム。

【請求項 7】前記ユーザデータとして、ユーザ ID が利用される請求項 1、請求項 2、請求項 3 又は請求項 4 記

載のデータ管理システム。

【請求項 8】前記ユーザデータとして、ユーザメールアドレスが利用される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 9】前記ユーザデータとして、前記ユーザの要求に対して生成された秘密鍵が利用される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 10】前記ユーザデータとして、データセンタ等がユーザ固有のものとして用意する乱数が利用される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 11】前記ユーザデータとして、前記データ管理センタがユーザ情報とユーザ公開鍵を組み合わせ得たデータを MD 5 ハッシュアルゴリズムによりハッシュ値化した MD 5 ハッシュ値が利用される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 12】秘密鍵が前記ユーザデータを利用して生成される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 13】秘密鍵が前記キーセンタのライブラリから選択される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 14】前記ユーザが前記キーセンタにユーザ公開鍵を提示して前記秘密鍵の配送を要求し；前記キーセンタが前記秘密鍵を前記ユーザ公開鍵を用いて暗号化して暗号化秘密鍵として前記ユーザに配送し；前記ユーザがユーザ専用鍵を用いて前記暗号化秘密鍵を復号して使用する請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 15】前記秘密鍵が 2 つの部分秘密鍵に分割され；前記 2 つの部分秘密鍵の一方が単独に配送され；前記 2 つの部分秘密鍵の他方が前記データコンテンツに添付されて配送される；請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 16】前記秘密鍵が IC カード中に自動的に保管される請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 17】前記秘密鍵が P C M C I A カード中に自動的に保管される請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 18】前記秘密鍵が挿入ボード中に自動的に保管される請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 19】前記秘密鍵がソフトウェア中に自動的に保管される請求項 1、請求項 2 又は請求項 3 記載のデータ管理システム。

【請求項 20】前記秘密鍵の上に次の秘密鍵が書き込まれることにより前記秘密鍵が破棄される請求項 1、請求

項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 1】前記電子透かしが、前記ユーザデータをデータセンタ公開鍵を用いて暗号化した暗号化ユーザデータである請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 2】前記秘密鍵の上に次の秘密鍵が書き込まれることにより前記秘密鍵が破棄される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 3】前記電子透かしが、前記ユーザデータである請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 4】前記電子透かしの上に次の電子透かしが書き込まれる請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 5】前記電子透かしに次の電子透かしが併記される請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 6】前記データコンテンツが公開の著作権付データコンテンツであり、前記秘密鍵が有料の鍵である請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 7】前記データコンテンツが非公開のデータコンテンツであり、前記秘密鍵が無料の鍵である請求項 1、請求項 2、請求項 3 又は請求項 4 記載のデータ管理システム。

【請求項 2 8】前記データ管理プログラムオブジェクトが IC カード中に格納されて供給される請求項 4 記載のデータ管理システム。

【請求項 2 9】前記データ管理プログラムオブジェクトが P C M C I A カード中に格納されて供給される請求項 4 記載のデータ管理システム。

【発明の詳細な説明】

【0001】

【利用分野】本発明はデジタルデータコンテンツの利用、保存、複写、加工、転送におけるデータ管理システムに係るものである。

【0002】

【先行技術】アナログデータコンテンツは保存、複写、加工、転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータコンテンツは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータコンテンツの著作権処理には的確な方法がなく、著作権法あるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0003】データコンテンツの利用法は単にその内容を参照するだけでなく、通常は得たデータコンテンツを保存、複写、加工することによって有効活用し、加工したデータコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオンラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータコンテンツとして登録することさえ可能である。従来のデータベースシステムにおいては文字データコンテンツのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータコンテンツに加えて、本来アナログデータコンテンツである音声データコンテンツ及び画像データコンテンツがデジタル化されてデータベースとされる。

【0004】このような状況において、データベース化されたデータコンテンツの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の 2 次利用について完成された著作権管理手段はない。本発明者らは特開平 6-46419 号及び特開平 6-1410004 号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平 6-132916 号でそのための装置を提案した。

【0005】また、特開平 7-271865 において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータコンテンツの表示（音声化を含む）、保存等の 1 次利用及び複写、加工、転送等の 2 次利用における著作権管理方法を提案した。

【0006】この先願のデータベース著作権管理システムでは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム、著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数をを用い、暗号化して転送されたデータコンテンツを復号して、視聴・加工の利用を行い、保存・複写・転送の利用を行う場合にデータコンテンツは再暗号化される。

【0007】著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムはデータコンテンツの復号化／暗号化を行うとともに申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0008】一方、企業内等の組織においてコンピュータを相互に接続して LAN (Local Area Network) を構成することが広く行われているが、複数のネットワークを相互に接続し、複数のネットワーク全体をあたかも 1 つのネットワークであるかのように利用するインターネット (Internet) が世界的な規模で構成されている。

【0009】企業内等の組織内のLANには組織外に知られてはならない秘密情報が保管されていることが多い。そのため、そのような秘密情報は特定のユーザのみが利用できるようにする必要があり、外部への秘密情報の漏洩を防止するために、一般的にはアクセスコントロールが行われる。アクセスコントロール方法には、大きく分けてアクセス許可によって行う方法と、暗号化によって行う方法の2種類の方法がある。

【0010】アクセス許可によるアクセスコントロール方法は、USP5173939、5220604、5224163、5315657、5438508に述べられている。暗号化によるアクセスコントロール方法は、USP5224163、5457746、5584023に述べられており、暗号化とデジタル署名によるアクセスコントロール方法が、USP4919545に述べられている。

【0011】また、複数のLANをインターネットを経由して接続しあっても単一のLANであるかのように利用するイントラネット(Intranet)が普及しつつある。このイントラネットにおいては本質的に窃取等に対する安全性を有しないインターネットを経由して情報交換を行うため、秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止することが、USP5515441に述べられており、その場合に複数の暗号鍵を用いることがUSP5504816、5353351、5475757及び5381480に述べられており、再暗号化を行うことがUSP5479514に述べられている。

【0012】暗号化する場合には、暗号鍵の受け渡しを含む暗号鍵管理が重要な問題となるが、暗号生成をICカードによって行うことがUSP5577121に、暗号化/復号化をICカードによって行うことがUSP5504817に各々述べられている。

【0013】これまでは従来の音声電話器にテレビジョン映像を付加したものに過ぎなかったテレビジョン会議システムが、最近ではコンピュータシステムに組み込まれることにより音声あるいは映像の品質が向上したばかりでなく、コンピュータ上のデータコンテンツも音声及び映像と同時に扱うことができるように進化している。このような中で、テレビジョン会議参加者以外の盗視聴による使用者のプライバシー侵害及びデータコンテンツの漏洩に対するセキュリティは秘密鍵を用いた暗号化システムによって保護されている。しかし、テレビジョン会議参加者自身が入手する会議内容は復号化されたものであるため、テレビジョン会議参加者自身が会議内容を保存し、場合によっては加工を行い、さらにはテレビジョン会議参加者以外の者に配送する2次的な利用が行われた場合には他のテレビジョン会議参加者のプライバシー及びデータコンテンツのセキュリティは全く無防備である。特に、伝送データコンテンツの圧縮技術が発達

する一方でデータ蓄積媒体の大容量化が進んだ結果テレビジョン会議の内容全てがデータ蓄積媒体に複写されたりあるいはネットワークを介して転送される虞れさえ現実のものとなりつつある。

【0014】また、デジタルデータコンテンツを商取引に利用する電子商取引システムが実現しつつあり、中でも現金に代えて電子データコンテンツを交換するデジタルキャッシュシステムは一般の人でも使用可能なシステムの完成を目標として種々の実験が進められている。これまでに種々提案されているデジタルキャッシュシステムは秘密鍵方式で暗号化デジタルキャッシュデータコンテンツを銀行預金口座あるいはクレジット会社のキャッシングサービスから転送してICカードに保存しており、入出力用の端末装置を利用して支払を行う。このICカードを電子財布として利用するデジタルキャッシュシステムは商店等入出力用の端末装置が設置されている場所であればどこでも使用可能である反面、入出力用の端末装置がない場所、例えば家庭等、では使用不可能である。

【0015】ところで、デジタルキャッシュは暗号化データコンテンツであるからICカード以外にも暗号化データコンテンツを保存することができ、かつ支払先にデータコンテンツを転送することができる装置であればどのようなものでもデジタルキャッシュデータコンテンツを保存する電子財布として利用することができる。具体的に電子財布として利用可能なユーザ端末装置としては、パーソナルコンピュータ、インテリジェントテレビジョン装置、携帯情報端末装置(Personal Digital Assistant PDA)、PHS(Personal Handyphone System)等の携帯電話器、インテリジェント電話機、入出力機能を有するPCカード等がある。

【0016】デジタルキャッシュは単なるデータコンテンツではなくデータコンテンツと機能が結びついたオブジェクト(object)として処理されることが望ましい。デジタルキャッシュの取り扱いにおいては共通のデジタルキャッシュフォーム、所有者固有の未記入デジタルキャッシュフォーム、所有者固有のデジタルキャッシュフォームの書き込み欄、金額であるデジタルキャッシュデータコンテンツ、デジタルキャッシュ取り扱いの指示、金額が書き込まれた所有者固有のデジタルキャッシュフォームがある。一方、オブジェクト指向プログラミング(object-oriented programming)においては、オブジェクト、クラス(class)、スロット(slot)、メッセージ(message)、インスタンス(instance)との概念が使用される。これらの対応関係は、共通のデジタルキャッシュフォームがオブジェクトとなり、所有者固有の未記入デジタルキャッシュフォームがクラスとなり、所有者固有のデジタルキャッシュフォームの記入欄がスロットとなり、デジタルキャッシュ取り扱いの指示がメッセージとなり、金額が記入された所有者固有のデジタルキャッシュフォ

ームがインスタンスとなる。金額等からなるデジタルキャッシュデータコンテンツは引数(argument)として使用され、メッセージによりインスタンス変数(instance variable)とも呼ばれるスロットに引き渡されて格納されることにより、金額等が更新されたデジタルキャッシュである新しいインスタンスが作られる。データ管理システムで利用される暗号技術は著作権データコンテンツの流通だけではなくデジタルキャッシュの流通に対しても利用されている。

【0017】先行技術の最後に本発明で利用する基本的な暗号関連技術について説明する。

【暗号鍵】秘密鍵(secret key)システムは暗号化と復号化が同じ鍵で行れるため「共通鍵システム」とも呼ばれ、鍵を秘密にしておく必要があることから「秘密鍵システム」と呼ばれる。秘密鍵を用いる暗号アルゴリズムとして代表的なものに米国標準局(National Bureau of Standards)のDES(Data Encryption Standard)システム、日本電信電話のFEAL(Fast Encryption Algorithm)システム、三菱電機のMISTYシステムがある。以下説明する実施例において秘密鍵を「Ks」と表示する。

【0018】これに対して公開鍵システムは、公開されている公開鍵(public key)とその鍵の所有者以外には秘密にされている専用鍵(private key)を用い、一方の鍵で暗号化し他方の鍵で復号化する暗号システムであり、代表的なものにRSA公開鍵システムがある。以下説明する実施例において公開鍵を「Kb」と、専用鍵を「Kv」と表示する。このときに、平文データコンテンツM(Material)を秘密鍵Ksを用いた暗号文Cks(Cryptogram)に暗号化(Encryption)する操作を、

$$Cks = E(M, Ks)$$

暗号文Cksを暗号鍵Ksを用いて平文データコンテンツMに復号化(Decryption)する操作を、

$$M = D(Cks, Ks)$$

また、平文データコンテンツMを公開鍵Kbを用いて暗号文Ckbに暗号化する操作を、

$$Ckb = E(M, Kb)$$

暗号文Ckbを専用鍵Kvを用いて平文データコンテンツMに復号化する操作を、

$$M = D(Ckv, Kv)$$

と、平文データコンテンツMを専用鍵Kvを用いて暗号文Ckvに暗号化する操作を、

$$Ckv = E(M, Kv)$$

暗号文Ckvを公開鍵Kbを用いて平文データコンテンツMに復号化する操作を、

$$M = D(Ckb, Kb)$$

と表現する。

【0019】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定

することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス683号、p.99~124に「電子透かし」がマルチメディア時代を守る(1997/2/24, 日経BP社刊)に全般的に紹介されており、また同号、p.149~162、ウォルター ベンダー他「電子透かしを支えるデータ・ハイディング技術(上)」及び684号、p.155~168、「電子透かしを支えるデータ・ハイディング技術(下)」(IBM System Journal, vol.35, nos.3 & 4(International Business Machines Corporation)から転載)にも紹介されている。

【0020】

【発明の概要】データコンテンツの盗用あるいは漏洩を防止するために、暗号技術と電子透かし技術を組み合わせて使用する。第1ユーザに供給されるデータコンテンツにはデータ管理センタによって第1ユーザデータが電子透かしとして埋め込まれ、電子透かしが埋め込まれたデータコンテンツが暗号鍵を用いて暗号化されて供給される。暗号化データコンテンツはデータ管理センタから配送される暗号鍵を用いて復号して利用され、保存する場合には別の暗号鍵を用いて暗号化される。データコンテンツを第2ユーザに複写・転送する場合には第2ユーザのユーザデータが電子透かしとして埋め込まれ、第2ユーザのユーザデータを電子透かしを埋め込むシナリオがデータ管理センタに登録され、電子透かしが埋め込まれたデータコンテンツが別の暗号鍵を用いて暗号化されて供給される。シナリオによって第2ユーザの正当性が確認されると、第2ユーザに別の暗号鍵が配送され、暗号化データコンテンツは別の暗号鍵を用いて復号して利用され、保存する場合にはさらに別の暗号鍵を用いて暗号化される。

【0021】第1ユーザが入手したデータにはデータセンタの手により、第1ユーザデータが電子透かしとして埋め込まれているので、正規の手続きによらずに複写・転送が行われた場合には、データセンタがそこに埋め込まれている電子透かしを検証することにより、正規の手続きによらずに複写・転送を行った第1ユーザを発見することができる。正規の手続きによって複写・転送が行われた場合のデータには各ユーザの電子透かしが埋め込まれているため、複写・転送の経路が明瞭になり、複写・転送が繰り返されると埋め込まれた電子透かしによりデータ中のノイズが増えるため、不正利用の危険性が増える複写・転送を抑制することができる。

【0022】また、キーセンタにはデータコンテンツの暗号化に使用された鍵が保存されているから、鍵預託システム(Key Escrow System)あるいは鍵回復システム(Key Recovery System)を実現する場合にこのキーセン

タを利用することができる。さらに、ユーザデータとして秘密鍵を利用し、この秘密鍵をデータセンタの公開鍵を用いて暗号化したものを電子透かしとして埋め込んでおき、必要な場合にはデータセンタの専用鍵によって復号して秘密鍵の確認を行うことにより、簡易でありながら安全性が高い鍵預託システムあるいは鍵回復システムを実現することができる。

【0023】この発明は有料の暗号鍵を使用するデータコンテンツの著作権管理の他に、無料の暗号鍵を使用するテレビジョン会議システムにおけるテレビジョン会議参加者のプライバシー確保及びデータコンテンツのセキュリティ確保、あるいは電子商取引等の電子データ交換 (Electronic Data Interchange: EDI) におけるデータセキュリティの確保にも応用可能される。

【0024】

【実施例】

【実施例1】図1を用いて、第1実施例を説明する。

(1) データセンタとキーセンタからデータ管理センタが構成されるが、これらは別個の組織であってもよい。また、データ管理センタ内のデータセンタは、IPのデータコンテンツM0をデータベースに予め保存しておくか、あるいは第1ユーザU1の要求に対応してその都度IPからデータコンテンツM0を転送してもらう。

【0025】(2) 第1ユーザU1はキーセンタに、データコンテンツ名Tmを指定し、ユーザデータI1及び第1ユーザの公開鍵Kb1を提示し、復号用の秘密鍵Ks1及び再暗号用の秘密鍵Ks2の配送を要求する。なお、ユーザデータとしては、ユーザID、ユーザE-mailアドレス等あるいはユーザの秘密鍵要求に対して生成される秘密鍵が利用可能であり、さらにデータセンタ等がユーザ固有のものとして用意する乱数等が利用可能である。また、データ管理センタが通常数十バイト程度のデータ量である第1ユーザ情報と同じく1000ビット程度のデータ量である第1ユーザ公開鍵Kb1を組み合わせる千数百ビット程度のデータ量である第1ユーザデータI1を得、この第1ユーザデータI1をMD5ハッシュアルゴリズムによりハッシュ値化した16バイトのMD5ハッシュ値をユーザデータとして使用することもできる。

【0026】(3) キーセンタは、秘密鍵Ks1及びKs2を生成しデータコンテンツ名Tm0、第1ユーザデータI1及び第1ユーザの公開鍵Kb1とともに保管し、秘密鍵Ks1及びKs2を第1ユーザの公開鍵Kb1を用いて暗号化し、

$$Cks1kb1 = E(Ks1, Kb1)$$

$$Cks2kb1 = E(Ks2, Kb1)$$

暗号化秘密鍵Cks1kb1及びCks2kb1を第1ユーザに配送する。

【0027】(4) 第1ユーザU1は配送された暗号化秘密鍵Cks1kb1及びCks2kb1を、第1ユーザの専用鍵Kv1を用いて復号し、

$$Ks1 = D(Cks1kb1, Kv1)$$

$$Ks2 = D(Cks2kb1, Kv1)$$

復号された秘密鍵Ks1及びKs2を装置内に保管するが、秘密鍵Ks1及びKs2の所有者はユーザではなくキーセンタあるいはデータセンタであり、秘密鍵の管理をユーザに行わせることには悪用の可能性もあるため、秘密鍵Ks1及びKs2の管理はユーザが管理することができないICカード、PCMCIAカード、挿入ボードあるいはソフトウェア中に自動的に保管される。

10 【0028】なお、このときに、データコンテンツM0使用料の課金が行われる。秘密鍵Ks1及びKs2の生成は、第1ユーザデータI1を利用して行うことができる。この場合にはデータコンテンツ名と第1ユーザデータI1があれば、Ks1を再生成することが可能であるから、保管するのはデータコンテンツ名Tm0、第1ユーザデータI1及び第1ユーザの公開鍵Kb1でよい。秘密鍵は生成するのではなく、キーセンタのライブラリからその都度選択するようにしてもよい。

20 【0029】また、本発明者の出願である特開平7-271865号に著作権管理プログラムを分割して各々データコンテンツと鍵に添付して配送する方法が述べられているが、この方法を秘密鍵自身に適用し、秘密鍵Ks1を

$$Ks21 + Ks22 = Ks2$$

として部分秘密鍵Ks11とKs12に、また秘密鍵Ks1を $Ks21 + Ks22 = \text{秘密鍵 } Ks2$

30 として部分秘密鍵Ks11とKs12に各々分割し、部分秘密鍵Ks11と部分秘密鍵Ks21を部分秘密鍵として、残りの部分秘密鍵Ks12と部分秘密鍵Ks22をデータコンテンツに添付して配送するようにすることにより、秘密鍵Ks1及びKs2の管理を第1ユーザが行うことはできなくなる。

【0030】(5) 第1ユーザU1が第1ユーザデータI1を提示し、データコンテンツ名Tm0を指定してデータセンタにデータコンテンツM0の配送を要求する。

40 【0031】(6) データセンタは、第1ユーザが提示した第1ユーザデータI1及びデータコンテンツ名Tm0をキーセンタに転送し、秘密鍵Ks1及びKs2の転送を依頼する。(7) キーセンタは、秘密鍵Ks1及びKs2をデータセンタに転送する。

【0032】(8) データセンタは、第1ユーザデータI1をデータセンタの公開鍵Kb0を用いて暗号化して $Cilk0 = E(I1, Kb0)$

50 暗号化第1ユーザデータCilk0とし、第1ユーザU1が要求するデータコンテンツM0に暗号化第1ユーザデータCilk0を電子透かしWcilk0として埋め込んで $M1 = M0 + Wcilk0$

電子透かし付データコンテンツM1に加Tし、電子透かし付データコンテンツM1を秘密鍵Ks1を用いて暗号化して

$Cm1ks1 = E(M1, Ks1)$

暗号化電子透かし付データコンテンツ $Cm1ks1$ とし、データ通信あるいはデータ放送により、ないしは媒体に記録して第1ユーザ $U1$ に配送する。また、データコンテンツ $M1$ の加工プロセス（第1ユーザデータ等電子透かしに関する情報）のシナリオは検証に用いるため保管される。なお、簡易形式として電子透かしとして暗号化第1ユーザデータ $Ci1kb0$ ではなく、第1ユーザデータ $I1$ を電子透かし $Wi1$ として埋め込むようにしてもよい。

【0033】(9) 第1ユーザ $U1$ は、暗号化電子透かし付データコンテンツ $Cm1ks1$ を復号用の秘密鍵 $Ks1$ を用いて復号して、

$M1 = D(Cm1ks1, Ks1)$

利用する。この時に秘密鍵 $Ks1$ の上に秘密鍵 $Ks2$ が上書きされる等の方法により秘密鍵 $Ks1$ は破棄される。

【0034】(10) データコンテンツ $M1$ が保存装置内に再保存される際には、データコンテンツ $M1$ が再暗号用の秘密鍵 $Ks2$ を用いて再暗号化されて、

$Cm1ks2 = E(M1, Ks2)$

再暗号化データコンテンツ $Cm1ks2$ として保存される。

【0035】(11) 第1ユーザ $U1$ が再暗号化データコンテンツ $Cm1ks2$ の再利用をする場合には、第1ユーザ $U1$ は、保存装置内に保存されている再暗号化データコンテンツ $Cm1ks2$ をメモリ上に読み出し、秘密鍵 $Ks2$ を用いて復号して利用し、第1ユーザがデータコンテンツ $M2$ を再保存する際には、再暗号用の秘密鍵 $Ks2$ を用いてデータコンテンツ $M1$ を再暗号化し、再暗号化データコンテンツ $Cm1ks2$ を保存装置内に保存する。

【0036】(12) 第1ユーザが第2ユーザ $U2$ にデータコンテンツ $M1$ を転送する場合には、第1ユーザ $U1$ は、第2ユーザデータ $I2$ をデータセンタの公開鍵 $Kb0$ を用いて暗号化し、

$Ci2kb0 = E(I2, Kb0)$

暗号化第2ユーザデータ $Ci2kb0$ を第2ユーザ $U2$ が要求するデータコンテンツ $M1$ に電子透かし $Wci2kb0$ として埋め込んで、

$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0$

電子透かし付データコンテンツ $M2$ に加工する。なお、簡易形式として電子透かしとして暗号化第2ユーザデータ $Ci2kb0$ ではなく、第2ユーザデータ $I2$ を電子透かし $Wi2$ として埋め込むようにしてもよい。

【0037】(13) 電子透かし付データコンテンツ $M1$ を電子透かし付データコンテンツ $M2$ に加工した第1ユーザ $U1$ は、加工されたデータコンテンツ $M2$ の加工プロセス（第2ユーザデータ等電子透かしに関する情報）のシナリオをキーセンタに転送し、登録することにより第2ユーザのデータコンテンツ利用が可能となる。

【0038】(14) さらに、第1ユーザ $U1$ は電子透かし付データコンテンツ $M2$ を秘密鍵 $Ks2$ を用いて暗号化して、

$Cm2ks2 = E(M2, Ks2)$

暗号化電子透かし付データコンテンツ $Cm2ks2$ を得る。

【0039】(15) 第1ユーザ $U1$ は、暗号化電子透かし付データコンテンツ $Cm2ks2$ をデータ通信あるいは媒体への複写により第2ユーザ $U2$ に転送する。

【0040】(16) 第2ユーザ $U2$ は転送された暗号化データコンテンツ $Cm2ks2$ を保存装置内に保存する。第2ユーザ $U2$ はキーセンタに、データコンテンツ名 Tm を指定し、第2ユーザの公開鍵 $Kb2$ を提示し、復号用の秘密鍵 $Ks2$ 及び再暗号用の秘密鍵 $Ks3$ の配送を要求する。

【0041】(17) キーセンタは、保管されていたシナリオによって第2ユーザ $U2$ が正当なユーザであることを確認し、秘密鍵 $Ks3$ を生成し保管するとともに、保存されていた秘密鍵 $Ks2$ 及び生成された秘密鍵 $Ks3$ を第2ユーザの公開鍵 $Kb2$ を用いて暗号化し、

$Cks2kb2 = E(Ks2, Kb2)$

$Cks3kb2 = E(Ks3, Kb2)$

暗号化秘密鍵 $Cks2kb2$ 及び暗号化秘密鍵 $Cks3kb2$ を第2ユーザに配送する。

【0042】(18) 第2ユーザ $U2$ は、第2ユーザの専用鍵 $Kv2$ を用いて暗号化秘密鍵 $Cks2kb2$ 及び暗号化秘密鍵 $Cks3kb2$ を復号し、

$Ks2 = D(Cks2kb2, Kb2)$

$Ks3 = D(Cks3kb2, Kb2)$

復号された秘密鍵 $Ks2$ 及び $Ks3$ はICカード、PCMCIAカード、挿入ボードあるいはソフトウェア中に保管される。なお、第2ユーザにおける秘密鍵 $Ks2$ 及び $Ks3$ には第1ユーザにおける秘密鍵 $Ks1$ 及び $Ks2$ と同様な取り扱いがなされて復号・保存がなされる。

【0043】(19) 第2ユーザ $U2$ は、保存装置内に保存されている暗号化電子透かし付データコンテンツ $Cm2ks2$ をメモリ上に読み出し、保存されていた秘密鍵 $Ks2$ を用いて復号して、

$M2 = D(Cm2ks2, Ks2)$

利用する。この時に秘密鍵 $Ks2$ の保管場所に秘密鍵 $Ks3$ が上書きされること等の方法により秘密鍵 $Ks2$ は破棄される。

【0044】(20) データコンテンツ $M2$ が保存装置内に再保存される際には、データコンテンツ $M2$ が再暗号用の秘密鍵 $Ks3$ を用いて再暗号化されて再暗号化データコンテンツ $Cm2ks3$ として保存される。

【0045】(21) 第2ユーザ $U2$ が再暗号化データコンテンツ $Cm2ks3$ の再利用をする場合には、保存装置内に保存されている再暗号化データコンテンツ $Cm2ks3$ をメモリ上に読み出し、秘密鍵 $Ks3$ を用いて復号して利用する。

【0046】(22) 第2ユーザがデータコンテンツ $M2$ を再保存する際には、再暗号用の秘密鍵 $Ks3$ を用いてデータコンテンツ $M2$ を再暗号化し、再暗号化データコンテンツ $Cm2ks3$ を保存装置内に保存する。以後、同様な動

作が繰り返される。

【0047】以上説明した実施例は、配送されるデータコンテンツをリアルタイムで利用することを前提にして構成されているが、ユーザが予め入手して保存していたデータコンテンツを後で復号利用する構成もありうる。その場合は第1ユーザが上記実施例の第2ユーザの立場に置かれて、同様な動作が行われる。

【0048】以上の説明から明らかなように、第1ユーザが入手したデータコンテンツにはデータセンタの手により、第1ユーザデータが電子透かしとして埋め込まれている。したがって、正規の手続きによらずに複写・転送が行われた場合には、データセンタがそこに埋め込まれている電子透かしを検証することにより、正規の手続きによらずに複写・転送を行った第1ユーザを発見することができる。正規の手続きによって複写・転送が行われた場合のデータコンテンツには各ユーザの電子透かしが埋め込まれているため、複写・転送の経路が明瞭になり、複写・転送が繰り返されると埋め込まれた電子透かしによりデータコンテンツ中のノイズが増えるため、不正規利用の危険性が増える複写・転送を抑制することができる。

【0049】また、キーセンタにはデータコンテンツの暗号化に使用された鍵が保存されているから、鍵預託システム(Key Escrow System)あるいは鍵回復システム(Key Recovery System)を実現する場合にこのキーセンタを利用することができる。

【0050】さらに、ユーザデータとして秘密鍵を利用し、この秘密鍵をデータセンタの公開鍵を用いて暗号化したものを電子透かしとして埋め込んでおき、必要な場合にはデータセンタの専用鍵によって復号して秘密鍵の確認を行うことにより、簡易でありながら安全性が高い鍵預託システムあるいは鍵回復システムを実現することができる。

【0051】〔実施例2〕図2を用いて、第2実施例を説明する。

(1) データセンタとキーセンタからデータ管理センタが構成されるが、これらは別個の組織であってもよい。また、データ管理センタ内のデータセンタは、IPのデータコンテンツM0をデータベースに予め保存しておくか、あるいは第1ユーザUIの要求に対応してその都度IPからデータコンテンツM0を転送してもらう。

【0052】(2) 第1ユーザUIはキーセンタに、データコンテンツ名Tm0を指定し、ユーザデータI1及び第1ユーザの公開鍵Kb1を提示し、復号用の秘密鍵Ks1及び再暗号用の秘密鍵Ks2の配送を要求する。このときに、データコンテンツM0使用料の課金が行われる。なお、ユーザデータとしては、ユーザID、ユーザE-mailアドレス等あるいはユーザの秘密鍵要求に対して生成される秘密鍵が利用可能であり、さらにデータセンタ等がユーザ固有のものとして用意する乱数等が利用可能であ

る。また、データ管理センタが通常数十バイト程度のデータ量である第1ユーザ情報と同じく1000ビット程度のデータ量である第1ユーザ公開鍵Kb1を組み合わせる千数百ビット程度のデータ量である第1ユーザデータI1を得、この第1ユーザデータI1をMD5ハッシュアルゴリズムによりハッシュ値化した16バイトのMD5ハッシュ値をユーザデータとして使用することもできる。

【0053】(3) キーセンタは、秘密鍵Ks1及びKs2を生成しデータコンテンツ名Tm0、第1ユーザデータI1及び第1ユーザの公開鍵Kb1とともに保管し、秘密鍵Ks1及びKs2を第1ユーザの公開鍵Kb1を用いて暗号化し、

$$Cks1kb1 = E(Ks1, Kb1)$$

$$Cks2kb1 = E(Ks2, Kb1)$$

暗号化秘密鍵Cks1kb1及びCks2kb1を第1ユーザに配送する。

【0054】(4) 第1ユーザUIは配送された暗号化秘密鍵Cks1kb1及びCks2kb1を、第1ユーザの専用鍵Kv1を用いて復号し、

$$Ks1 = D(Cks1kb1, Kv1)$$

$$Ks2 = D(Cks2kb1, Kv1)$$

復号された秘密鍵Ks1及びKs2を装置内に保管するが、秘密鍵Ks1及びKs2の所有者はユーザではなくキーセンタあるいはデータセンタであり、秘密鍵の管理をユーザに行わせることには悪用の可能性もあるため、秘密鍵Ks1及びKs2の管理はユーザが管理することができないICカード、PCMCIAカード、挿入ボードあるいはソフトウェア中に自動的に保管される。

【0055】なお、このときに、データコンテンツM0使用料の課金が行われる。秘密鍵Ks1及びKs2の生成は、第1ユーザデータI1を利用して行うことができる。この場合にはデータコンテンツ名と第1ユーザデータI1があれば、Ks1を再生成することが可能であるから、保管するのはデータコンテンツ名Tm0及び第1ユーザデータI1及び第1ユーザの公開鍵Kb1でよい。秘密鍵は生成するのではなく、キーセンタのライブラリからその都度選択するようにしてもよい。

【0056】また、本発明者の出願である特開平7-271865号に著作権管理プログラムを分割して各々データコンテンツと鍵に添付して配送する方法が述べられているが、この方法を秘密鍵自身に適用し、秘密鍵Ks1を

$$Ks21 + Ks22 = Ks2$$

として部分秘密鍵Ks11とKs12に、また秘密鍵Ks1をKs21 + Ks22 = 秘密鍵Ks2

として部分秘密鍵Ks11とKs12に各々分割し、部分秘密鍵Ks11と部分秘密鍵Ks21を部分秘密鍵として、残りの部分秘密鍵Ks12と部分秘密鍵Ks22をデータコンテンツに添付して配送するようにすることにより、秘密鍵Ks1

及びKs2の管理を第1ユーザが行うことはできなくなる。

【0057】(5) 第1ユーザU1が第1ユーザデータI1を提示し、データコンテンツ名Tm0を指定してデータセンタにデータコンテンツM0の配送を要求する。

【0058】(6) データセンタは、第1ユーザが提示した第1ユーザデータI1及びデータコンテンツ名Tm0をキーセンタに転送し、秘密鍵Ks1及びKs2の転送を依頼する。

(7) キーセンタは、秘密鍵Ks1及びKs2をデータセンタに転送する。

【0059】(8) データセンタは、第1ユーザデータI1をデータセンタの公開鍵Kb0を用いて暗号化して $Ci1kb0 = E(I1, Kb0)$

暗号化第1ユーザデータCi1kb0とし、第1ユーザU1が要求するデータコンテンツM0に暗号化第1ユーザデータCi1kb0を電子透かしWci1kb0として埋め込んで

$$M1 = M0 + Wci1kb0$$

電子透かし付データコンテンツM1に加工し、電子透かし付データコンテンツM1を秘密鍵Ks1を用いて暗号化して

$$Cm1ks1 = E(M1, Ks1)$$

暗号化電子透かし付データコンテンツCm1ks1とし、データ通信あるいはデータ放送により、ないしは媒体に記録して第1ユーザU1に配送する。また、データコンテンツM1の加工プロセス(第1ユーザデータ等電子透かしに関する情報)のシナリオは検証に用いるため保管される。なお、簡易形式として電子透かしとして暗号化第1ユーザデータCi1kb0ではなく、第1ユーザデータI1を電子透かしWi1として埋め込むようにしてもよい。

【0060】(9) 第1ユーザU1は、暗号化電子透かし付データコンテンツCm1ks1を復号用の秘密鍵Ks1を用いて復号して、

$$M1 = D(Cm1ks1, Ks1)$$

利用する。この時に秘密鍵Ks1の上に秘密鍵Ks2が上書きされる等の方法により秘密鍵Ks1は破棄される。

【0061】(10) データコンテンツM1が保存装置内に再保存される際には、データコンテンツM1が再暗号用の秘密鍵Ks2を用いて再暗号化されて、

$$Cm1ks2 = E(M1, Ks2)$$

再暗号化データコンテンツCm1ks2として保存される。

【0062】(11) 第1ユーザU1が再暗号化データコンテンツCm1ks2の再利用をする場合には、第1ユーザU1は、保存装置内に保存されている再暗号化データコンテンツCm1ks2をメモリ上に読み出し、秘密鍵Ks2を用いて復号して利用し、第1ユーザがデータコンテンツM2を再保存する際には、再暗号用の秘密鍵Ks2を用いてデータコンテンツM1を再暗号化し、再暗号化データコンテンツCm1ks2を保存装置内に保存する。

【0063】(12) 第1ユーザが第2ユーザU2にデータ

コンテンツM1を転送する場合には、第1ユーザU1は、第2ユーザデータI2をデータセンタの公開鍵Kb0を用いて暗号化し、

$$Ci2kb0 = E(I2, Kb0)$$

暗号化第2ユーザデータCi2kb0を第2ユーザU2が要求するデータコンテンツM1に電子透かしWci2kb0として埋め込んで、

$$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0$$

電子透かし付データコンテンツM2に加工する。なお、簡易形式として電子透かしとして暗号化第2ユーザデータCi2kb0ではなく、第2ユーザデータI2を電子透かしWi2として埋め込むようにしてもよい。

【0064】(13) 電子透かし付データコンテンツM1を電子透かし付データコンテンツM2に加工した第1ユーザU1は、加工されたデータコンテンツM2の加工プロセス(第2ユーザデータ等電子透かしに関する情報)のシナリオをキーセンタに転送し、登録することにより第2ユーザのデータコンテンツ利用が可能となる。

【0065】(14) キーセンタは、第1ユーザにより登録された加工プロセスのシナリオを保管するとともに、秘密鍵Ks3を生成し、第1ユーザの公開鍵Kb1を用いて暗号化し、

$$Cks3kb1 = E(Ks3, Kb1)$$

暗号化秘密鍵Cks3kb1を第1ユーザに配送する。

【0066】(15) 第1ユーザU1は配送された暗号化秘密鍵Cks3kb1を、第1ユーザの専用鍵Kv1を用いて復号する。

$$Ks3 = D(Cks3kb1, Kv1)$$

【0067】(16) さらに、電子透かし付データコンテンツM2を復号された秘密鍵Ks3を用いて暗号化して、

$$Cm2ks3 = E(M2, Ks3)$$

暗号化電子透かし付データコンテンツCm2ks3を得る。

【0068】(17) 第1ユーザU1は、暗号化電子透かし付データコンテンツCm2ks3をデータ通信あるいは媒体への複写により第2ユーザU2に転送する。

【0069】(18) 第2ユーザU2は転送された暗号化データコンテンツCm2ks3を保存装置内に保存する。第2ユーザU2はキーセンタに、データコンテンツ名Tm0を指定し、第2ユーザの公開鍵Kb2を提示し、復号用の秘密鍵Ks3及び再暗号用の秘密鍵Ks4の配送を要求する。

【0070】(19) キーセンタは、保管されていたシナリオにより第2ユーザU2が正当なユーザであることを確認し、秘密鍵Ks4を生成し保管するとともに、保存されていた秘密鍵Ks3を第2ユーザの公開鍵Kb2を用いて暗号化し、

$$Cks3kb2 = E(Ks3, Kb2)$$

$$Cks4kb2 = E(Ks4, Kb2)$$

暗号化秘密鍵Cks3kb2及び暗号化秘密鍵Cks4kb2を第2ユーザに配送する。

【0071】(20) 第2ユーザU2は、第2ユーザの専用

鍵 $Kv2$ を用いて暗号化秘密鍵 $Cks3kb2$ 及び暗号化秘密鍵 $Cks4kb2$ を復号し、

$Ks3 = D(Cks3kb2, Kv2)$

$Ks4 = D(Cks4kb2, Kv2)$

復号された秘密鍵 $Ks3$ 及び $Ks4$ は IC カード、PCMCIA カード、挿入ボードあるいはソフトウェア中に保管される。なお、第 2 ユーザにおける秘密鍵 $Ks3$ 及び $Ks4$ には第 1 ユーザにおける秘密鍵 $Ks1$ 及び $Ks2$ と同様な取り扱いがなされる。

【0072】(21) 第 2 ユーザ $U2$ は、保存装置内に保存されている暗号化電子透かし付データコンテンツ $Cm2ks3$ をメモリ上に読み出し、保存されていた秘密鍵 $Ks3$ を用いて復号して、

$M2 = D(Cm2ks3, Ks3)$

利用する。この時に秘密鍵 $Ks3$ の保管場所に秘密鍵 $Ks4$ が上書きされること等の方法により秘密鍵 $Ks3$ は破棄される。

【0073】(22) データコンテンツ $M2$ が保存装置内に再保存される際には、データコンテンツ $M2$ が再暗号用の秘密鍵 $Ks4$ を用いて再暗号化されて再暗号化データコンテンツ $Cm2ks4$ として保存される。

【0074】(23) 第 2 ユーザ $U2$ が再暗号化データコンテンツ $Cm2ks4$ の再利用をする場合には、保存装置内に保存されている再暗号化データコンテンツ $Cm2ks4$ をメモリ上に読み出し、秘密鍵 $Ks4$ を用いて復号して利用する。

【0075】(24) 第 2 ユーザがデータコンテンツ $M2$ を再保存する際には、再暗号用の秘密鍵 $Ks4$ を用いてデータコンテンツ $M2$ を再暗号化し、再暗号化データコンテンツ $Cm2ks4$ を保存装置内に保存する。以後、同様な動作が繰り返される。

【0076】以上説明した実施例は、配送されるデータコンテンツをリアルタイムで利用することを前提にして構成されているが、ユーザが予め入手して保存していたデータコンテンツを後で復号利用する構成もありうる。その場合は第 1 ユーザが上記実施例の第 2 ユーザの立場に置かれて、同様な動作が行われる。

【0077】以上の説明から明らかなように、第 1 ユーザが入手したデータコンテンツにはデータセンタの手により、第 1 ユーザデータが電子透かしとして埋め込まれている。したがって、正規の手続きによらずに複写・転送が行われた場合には、データセンタがそこに埋め込まれている電子透かしを検証することにより、正規の手続きによらずに複写・転送を行った第 1 ユーザを発見することができる。正規の手続きによって複写・転送が行われた場合のデータコンテンツには各ユーザの電子透かしが埋め込まれているため、複写・転送の経路が明瞭になり、複写・転送が繰り返されると埋め込まれた電子透かしによりデータコンテンツ中のノイズが増えるため、不正規利用の危険性が増える複写・転送を抑制することが

できる。

【0078】また、キーセンタにはデータコンテンツの暗号化に使用された鍵が保存されているから、鍵預託システム (Key Escrow System) あるいは鍵回復システム (Key Recovery System) を実現する場合にこのキーセンタを利用することができる。

【0079】さらに、ユーザデータとして秘密鍵を利用し、この秘密鍵をデータセンタの公開鍵を用いて暗号化したものを電子透かしとして埋め込んでおき、必要な場合にはデータセンタの専用鍵によって復号して秘密鍵の確認を行うことにより、簡易でありながら安全性が高い鍵預託システムあるいは鍵回復システムを実現することができる。

【0080】〔第 3 実施例〕図 3 を用いて第 3 実施例を説明する。

(1) この実施例におけるデータセンタとキーセンタは第 1 実施例あるいは第 2 実施例の場合と異なり、ユーザから見た場合に単一のデータ管理センタであるように構成されている。また、データ管理センタは、IP のデータコンテンツ $M0$ をデータベースに予め保存しておくか、あるいは第 1 ユーザ $U1$ の要求に対応してその都度 IP からデータコンテンツ $M0$ を転送してもらう。

【0081】(2) 第 1 ユーザ $U1$ は、データ管理センタに第 1 ユーザデータ $I1$ 及び第 1 ユーザ公開鍵 $Kb1$ を提示し、データコンテンツ名 $Tm0$ を指定してデータコンテンツ $M0$ 及び第 1 秘密鍵、第 2 秘密鍵の転送を要求する。なお、ユーザデータとしては、ユーザ ID、ユーザ E-mail アドレス等あるいはユーザの秘密鍵要求に対して生成される秘密鍵が利用可能であり、さらにデータセンタ等がユーザ固有のものとして用意する乱数等が利用可能である。また、データ管理センタが通常数十バイト程度のデータ量である第 1 ユーザ情報と同じく 1000 ビット程度のデータ量である第 1 ユーザ公開鍵 $Kb1$ を組み合わせ千数百ビット程度のデータ量である第 1 ユーザデータ $I1$ を得、この第 1 ユーザデータ $I1$ を MD5 ハッシュアルゴリズムによりハッシュ値化した 16 バイトの MD5 ハッシュ値をユーザデータとして使用することもできる。

【0082】(3) データ管理センタは秘密鍵 $Ks1$ 及び $Ks2$ を生成するとともに、第 1 ユーザデータ $I1$ をデータセンタの公開鍵 $Kb0$ を用いて暗号化して

$Cilk0 = E(I1, Kb0)$

暗号化第 1 ユーザデータ $Cilk0$ とし、第 1 ユーザ $U1$ が要求するデータコンテンツ $M0$ に暗号化第 1 ユーザデータ $Cilk0$ を電子透かし $Wcilk0$ として埋め込んで

$M1 = M0 + Wcilk0$

電子透かし付データコンテンツ $M1$ に加工し、電子透かし付データコンテンツ $M1$ を秘密鍵 $Ks1$ を用いて暗号化して

$Cmlks1 = E(M1, Ks1)$

暗号化電子透かし付データコンテンツCmlks1とする。

【0083】(4) データ管理センタは生成された秘密鍵Ks1及びKs2をデータコンテンツ名Tm0、第1ユーザデータI1及び第1ユーザの公開鍵Kb1とを保管するとともに、秘密鍵Ks1及びKs2を第1ユーザの公開鍵Kb1を用いて暗号化し、

$$Cks1kb1 = E(Ks1, Kb1)$$

$$Cks2kb1 = E(Ks2, Kb1)$$

2個の暗号化秘密鍵と暗号化電子透かし付データコンテンツCmlks1をデータ通信あるいはデータ放送により、ないしは媒体に記録して第1ユーザU1に配送する。また、データコンテンツM1の加工プロセス（第1ユーザデータ等電子透かしに関する情報）のシナリオは検証に用いるため保管される。なお、簡易形式として電子透かしとして暗号化第1ユーザデータCi1kb0ではなく、第1ユーザデータI1を電子透かしWi1として埋め込むようにしてもよい。

【0084】(5) 第1ユーザU1は配送された暗号化秘密鍵Cks1kb1及びCks2kb1を、第1ユーザの専用鍵Kv1を用いて復号し、

$$Ks1 = D(Cks1kb1, Kv1)$$

$$Ks2 = D(Cks2kb1, Kv1)$$

復号された秘密鍵Ks1及びKs2を装置内に保管するが、秘密鍵Ks1及びKs2の所有者はキーセンタあるいはデータセンタでありユーザではなく、秘密鍵の管理をユーザに行わせることには悪用の可能性もあるため、秘密鍵Ks1及びKs2の管理はユーザが管理することができないICカード、PCMCIAカード、挿入ボードあるいはソフトウェア中に自動的に保管される。

【0085】なお、このときに、データコンテンツM0使用料の課金が行われる。秘密鍵Ks1及びKs2の生成は、第1ユーザデータI1を利用して行うことができる。この場合にはデータコンテンツ名と第1ユーザデータI1があれば、Ks1を再生成することが可能であるから、保管するのはデータコンテンツ名Tm0及び第1ユーザデータI1でよい。秘密鍵は生成するのではなく、キーセンタのライブラリからその都度選択するようにしてもよい。

【0086】また、本発明者の出願である特開平7-271865号に著作権管理プログラムを分割して各々データコンテンツと鍵に添付して配送する方法が述べられているが、この方法を秘密鍵自身に適用し、秘密鍵Ks1を

$$Ks21 + Ks22 = Ks2$$

として部分秘密鍵Ks11とKs12に、また秘密鍵Ks1をKs21 + Ks22 = 秘密鍵Ks2

として部分秘密鍵Ks11とKs12に各々分割し、部分秘密鍵Ks11と部分秘密鍵Ks21を部分秘密鍵として、残りの部分秘密鍵Ks12と部分秘密鍵Ks22をデータコンテンツに添付して配送するようにすることにより、秘密鍵Ks1

及びKs2の管理を第1ユーザが行うことはできなくなる。

【0087】(6) 第1ユーザU1は、暗号化電子透かし付データコンテンツCmlks1を復号用の秘密鍵Ks1を用いて復号して、

$$M1 = D(Cmlks1, Ks1)$$

利用する。この時に秘密鍵Ks1の上に秘密鍵Ks2が書き加えられる等の方法により秘密鍵Ks1は破棄される。

【0088】(7) データコンテンツM1が保存装置内に再保存される際には、データコンテンツM1が再暗号用の秘密鍵Ks2を用いて再暗号化されて、

$$Cmlks2 = E(M1, Ks2)$$

再暗号化データコンテンツCmlks2として保存される。

【0089】(8) 第1ユーザU1が再暗号化データコンテンツCmlks2の再利用をする場合には、第1ユーザU1は、保存装置内に保存されている再暗号化データコンテンツCmlks2をメモリ上に読み出し、秘密鍵Ks2を用いて復号して利用し、第1ユーザがデータコンテンツM2を再保存する際には、再暗号用の秘密鍵Ks2を用いてデータコンテンツM1を再暗号化し、再暗号化データコンテンツCmlks2を保存装置内に保存する。

【0090】(9) 第1ユーザが第2ユーザU2にデータコンテンツM1を転送する場合には、第1ユーザU1は、第2ユーザデータI2をデータセンタの公開鍵Kb0を用いて暗号化し、

$$Ci2kb0 = E(I2, Kb0)$$

暗号化第2ユーザデータCi2kb0を第2ユーザU2が要求するデータコンテンツM1に電子透かしWci2kb0として埋め込んで、

$$M2 = M1 + Wci2kb0 = (M0 + Wci1kb0) + Wci2kb0$$

電子透かし付データコンテンツM2に加工する。なお、簡易形式として電子透かしとして暗号化第2ユーザデータCi2kb0ではなく、第2ユーザデータI2を電子透かしWi2として埋め込むようにしてもよい。

【0091】(10) 電子透かし付データコンテンツM2に加工した第1ユーザU1は加工されたデータコンテンツM2の加工プロセス（第2ユーザデータ等電子透かしに関する情報）のシナリオをキーセンタに転送し、登録することにより第2ユーザのデータコンテンツ利用が可能となる。

【0092】(11) さらに、第1ユーザU1は電子透かし付データコンテンツM2を秘密鍵Ks2を用いて暗号化して、

$$Cm2ks2 = E(M2, Ks2)$$

暗号化電子透かし付データコンテンツCm2ks2を得る。

【0093】(12) 第1ユーザU1は、暗号化電子透かし付データコンテンツCm2ks2をデータ通信あるいは媒体への複写により第2ユーザU2に転送する。

【0094】(13) 第2ユーザU2は転送された暗号化データコンテンツCm2ks2を保存装置内に保存する。第2

ユーザU2はキーセンタに、データコンテンツ名Tm0を指定し、第2ユーザの公開鍵Kb2を提示し、復号用の秘密鍵Ks2及び再暗号用の秘密鍵Ks3の配送を要求する。

【0095】(14) キーセンタは、保管されていたシナリオによって第2ユーザU2が正当なユーザであることを確認し、秘密鍵Ks3を生成し保管するとともに、保存されていた秘密鍵Ks2及び生成された秘密鍵Ks3を第2ユーザの公開鍵Kb2を用いて暗号化し、

$Cks2kb2 = E(Ks2, Kb2)$

$Cks3kb2 = E(Ks3, Kb2)$

暗号化秘密鍵Cks2kb2及び暗号化秘密鍵Cks3kb2を第2ユーザに配送する。

【0096】(15) 第2ユーザU2は、第2ユーザの専用鍵Kv2を用いて暗号化秘密鍵Cks2kb2及び暗号化秘密鍵Cks3kb2を復号し、

$Ks2 = D(Cks2kb2, Kv2)$

$Ks3 = D(Cks3kb2, Kv2)$

復号された秘密鍵Ks2及びKs3はICカード、PCMCIAカード、挿入ボードあるいはソフトウェア中に保管される。なお、第2ユーザにおける秘密鍵Ks2及びKs3には第1ユーザにおける秘密鍵Ks1及びKs2と同様な取り扱いがなされて復号・保存がなされる。

【0097】(16) 第2ユーザU2は、保存装置内に保存されている暗号化電子透かし付データコンテンツCm2ks2をメモリ上に読み出し、保存されていた秘密鍵Ks2を用いて復号して、

$M2 = D(Cm2ks2, Ks2)$

利用する。この時に秘密鍵Ks2の保管場所に秘密鍵Ks3が上書きされること等の方法により秘密鍵Ks2は破棄される。

【0098】(17) データコンテンツM2が保存装置内に再保存される際には、データコンテンツM2が再暗号用の秘密鍵Ks3を用いて再暗号化されて再暗号化データコンテンツCm2ks3として保存される。

【0099】(18) 第2ユーザU2が再暗号化データコンテンツCm2ks3の再利用をする場合には、保存装置内に保存されている再暗号化データコンテンツCm2ks3をメモリ上に読み出し、秘密鍵Ks3を用いて復号して利用する。

【0100】(19) 第2ユーザがデータコンテンツM2を再保存する際には、再暗号用の秘密鍵Ks3を用いてデータコンテンツM2を再暗号化し、再暗号化データコンテンツCm2ks3を保存装置内に保存する。以後、同様な動作が繰り返される。

【0101】以上説明した実施例は、配送されるデータコンテンツをリアルタイムで利用することを前提にして構成されているが、ユーザが予め入手して保存していたデータコンテンツを後で復号利用する構成もありうる。その場合は第1ユーザが上記実施例の第2ユーザの立場に置かれて、同様な動作が行われる。

【0102】以上の説明から明らかなように、第1ユーザが入手したデータコンテンツにはデータセンタの手により、第1ユーザデータが電子透かしとして埋め込まれている。したがって、正規の手続きによらずに複写・転送が行われた場合には、データセンタがそこに埋め込まれている電子透かしを検証することにより、正規の手続きによらずに複写・転送を行った第1ユーザを発見することができる。正規の手続きによって複写・転送が行われた場合のデータコンテンツには各ユーザの電子透かしが埋め込まれているため、複写・転送の経路が明瞭になり、複写・転送が繰り返されると埋め込まれた電子透かしによりデータコンテンツ中のノイズが増えるため、不正規利用の危険性が増える複写・転送を抑制することができる。

【0103】また、キーセンタにはデータコンテンツの暗号化に使用された鍵が保存されているから、鍵預託システム(Key Escrow System)あるいは鍵回復システム(Key Recovery System)を実現する場合にこのキーセンタを利用することができる。

【0104】[実施例4] 図4及び図5を用いて、第4実施例を説明する。この実施例は、データ管理システム全体に関する実施例である第1～第3実施例とは異なり、ユーザ側でのデータ管理動作に関する実施例である。なお、図4に記載されたフローチャートは第1ユーザ側で行われる動作の例であり、図5に記載されたフローチャートは第2ユーザ側で行われる動作の例である。この実施例ではデータ管理プログラムはオブジェクトプログラムとして構成されており、ユーザデータ、秘密鍵はオブジェクトのスロットにインスタンス変数として格納される。

【0105】(1) 第1ユーザU1は、データコンテンツM0を第1秘密鍵Ks1を用いて暗号化した暗号化データコンテンツCm0ks1を入手する。暗号化データコンテンツの入手はネットワークを経由して、データ放送により、あるいは記録媒体により可能である。

【0106】(2) 暗号化データコンテンツCm0ks1を入手した第1ユーザU1は、第1秘密鍵Ks1がインスタンス変数としてスロットに格納されたデータ管理プログラムオブジェクトをデータ管理センタから入手する。データ管理プログラムオブジェクトはネットワークを経由して行われてもよいが、安全のためにはICカード等に格納されて供給されることが望ましい。

【0107】(3) 第1ユーザデータI1がデータ管理プログラムオブジェクトのスロットにインスタンス変数として格納される。

(4) 第1ユーザデータI1がデータ管理プログラムオブジェクトに格納済みであることが確認される。そうでない場合には(3)の第1ユーザデータI1をデータ管理プログラムオブジェクトに格納する動作が繰り返される。

【0108】(5) データ管理プログラムにより第1ユー

ザデータI1に基づく電子透かしパターンW1が生成される。

(6) 第1ユーザU1は、第1秘密鍵Ks1を用いて暗号化データコンテンツCm0ks1を復号するが、

$M0 = D(Cm0ks1, Ks1)$

復号されたデータコンテンツM0には直ちに電子透かしW1が埋め込む加工が行われ、データコンテンツM0はデータコンテンツM1となる。

【0109】(7) データ管理プログラムにより第2秘密鍵が生成される。

(8) 生成された第2秘密鍵が第1秘密鍵に上書きされることにより第1秘密鍵Ks1が廃棄され、第2秘密鍵Ks2が保存される。

(9) これらの動作が完了した後にデータコンテンツM1が利用される。利用されるデータコンテンツはデータ管理センタから入手したデータコンテンツM0ではなく、第1ユーザU1のデータI1が電子透かしとして埋め込まれたデータコンテンツM1であるが、外見上は変化のない電子透かしであるから利用上の支障は全くない。

【0110】(10) 第1ユーザU1が利用したデータコンテンツM1を保存装置に保存する時には、初めにデータ管理プログラムにより第2秘密鍵Ks2を用いてデータコンテンツM1が再暗号化される。

$Cm1ks2 = E(M1, Ks2)$

(11) 次に保存されるデータコンテンツM1が暗号化データコンテンツCm1ks2とされているか否かが確認され、暗号化されていない場合にはデータコンテンツの保存は行われず、(9)の段階に戻る。

(12) 保存されようとするデータコンテンツが暗号化データコンテンツCm1ks2であることが確認されると暗号化データコンテンツCm1ks2が保存装置に保存される。

【0111】(13) 第1ユーザU1が暗号化データコンテンツCm1ks2を第2ユーザU2に対して複写・転送することなく再度使用する場合には、

(14) 保存装置に保存されている暗号化データコンテンツCm1ks2を読み出し、

(15) データ管理プログラムにより第2秘密鍵Ks2を用いて暗号化データコンテンツCm1ks2を復号し、

$M1 = D(Cm1ks2, Ks2)$

(16) 復号されたデータコンテンツM1を利用する。

(17) 第1ユーザU1が再利用したデータコンテンツM1を保存装置に保存する時には、初めにデータ管理プログラムにより第2秘密鍵Ks2を用いてデータコンテンツM1が再暗号化されて保存される。

【0112】(18) 第1ユーザU1が暗号化データコンテンツCm1ks2を第2ユーザU2に対して複写・転送する場合には、暗号化データコンテンツCm1ks2を記録媒体に複写してあるいはネットワークを経由して行う。

【0113】(19) 第2ユーザU2は、暗号化データコンテンツCm1ks2をネットワークを経由してあるいは記録

媒体により入手する。

【0114】(20) 暗号化データコンテンツCm1ks2を入手した第2ユーザU1は、第2秘密鍵Ks2がインスタンス変数としてスロットに格納されたデータ管理プログラムオブジェクトをデータ管理センタから入手する。データ管理プログラムオブジェクトはネットワークを経由して行われてもよいが、安全のためにはICカード等に格納されて供給されることが望ましい

10 【0115】(21) 第2ユーザデータI2がデータ管理プログラムオブジェクトのスロットにインスタンス変数として格納される。

(22) 第2ユーザデータI2がデータ管理プログラムオブジェクトに格納済みであることが確認される。そうでない場合には(21)の第2ユーザデータI2をデータ管理プログラムオブジェクトに格納する動作が繰り返される。

【0116】(23) データ管理プログラムにより第2ユーザデータI2に基づく電子透かしパターンW2が生成される。

20 (24) 第2ユーザU2は、第2秘密鍵Ks2を用いて暗号化データコンテンツCm1ks2を復号するが、

$M1 = D(Cm1ks2, Ks2)$

復号されたデータコンテンツM1には直ちに電子透かしW2が埋め込む加工が行われ、データコンテンツM1はデータコンテンツM2となる。

【0117】(25) データ管理プログラムにより第3秘密鍵が生成される。

(26) 生成された第3秘密鍵が第2秘密鍵に上書きされることにより第2秘密鍵Ks2が廃棄され、第3秘密鍵Ks3が保存される。

30 (27) これらの動作が完了した後にデータコンテンツM2が利用される。利用されるデータコンテンツはデータ管理センタから入手したデータコンテンツM0ではなく、第2ユーザU2のデータI2が電子透かしとして埋め込まれたデータコンテンツM2であるが、外見上は変化のない電子透かしであるから利用上の支障は全くない。なお、電子透かしW2は電子透かしW1に上書きされることにより、データコンテンツM2に埋め込まれている電子透かしが常に単一であるようにして最終のユーザデータの電子透かしのみであるようにすることも、電子透かしW2を電子透かしW1に上書きすることなく併記し、データコンテンツM2に埋め込まれている電子透かしが増えるようにしてすべてのユーザデータの電子透かしであるようにすることも可能である。

【0118】(28) 第2ユーザU2が利用したデータコンテンツM2を保存装置に保存する時には、初めにデータ管理プログラムにより第3秘密鍵Ks3を用いてデータコンテンツM2が再暗号化される。

$Cm2ks3 = E(M2, Ks3)$

50 (29) 次に保存されるデータコンテンツM2が暗号化データコンテンツCm2ks3とされているか否かが確認され、

暗号化されていない場合にはデータコンテンツの保存は行われず、(27)の段階に戻る。

(30) 保存されようとするデータコンテンツが暗号化データコンテンツ $Cm2ks3$ であることが確認されると暗号化データコンテンツ $Cm2ks3$ が保存装置に保存される。

【0119】 (31) 第2ユーザ $U2$ が暗号化データコンテンツ $Cm2ks3$ を第3ユーザ $U3$ に対して複写・転送することなく再度使用する場合には、

(32) 保存装置に保存されている暗号化データコンテンツ $Cm2ks3$ を読み出し、

(33) データ管理プログラムにより第3秘密鍵 $Ks3$ を用いて暗号化データコンテンツ $Cm2ks3$ を復号し、

$M2 = D(Cm2ks3, Ks3)$

(34) 復号されたデータコンテンツ $M2$ を利用する。

(35) 第2ユーザ $U2$ が再利用したデータコンテンツ $M2$ を保存装置に保存する時には、初めにデータ管理プログラムにより第3秘密鍵 $Ks3$ を用いてデータコンテンツ $M2$ が再暗号化されて保存される。

【0120】 (36) 第2ユーザ $U2$ が暗号化データコンテンツ $Cm2ks3$ を第3ユーザ $U3$ に対して複写・転送する場合には、暗号化データコンテンツ $Cm2ks3$ を記録媒体に複写してあるいはネットワークを経由して行う。以後、同様な動作が繰り返される。

【0121】 これまでに説明した第1～第4実施例は何れもデータ管理センタの管理するデータの不正な使用を防止する、いいかえれば有償のデータのために有償の鍵を使用するためのものである。しかしながら、これらの構成におけるデータ管理センタをテレビジョン会議ホストに、1次ユーザをテレビジョン会議のゲストに、2次以降のユーザをテレビジョン会議のオブザーバに置き換えることにより、テレビジョン会議システムに適用することにより会議内容の漏洩を防止することができる。

【0122】 また、同じようにデータ管理センタを顧客側銀行に、1次ユーザを顧客に、2次ユーザを小売店に置き換えて、デジタルキャッシュシステムに適用することによりデジタルキャッシュシステムの安全性が向上する。

【0123】 これまでに説明したシステムを利用する各ユーザは予めデータ管理センタに登録をしておく必要があり、また、この登録の際にデータ管理プログラムがユーザに対して提供される。また、本発明においてはデータ M を利用するために第1秘密鍵 $Ks1$ 、第2秘密鍵 $Ks2$ 及びデータ管理プログラムが各ユーザに対して転送され、各ユーザはこれらを保管しておく必要がある。これらの保管場所としては、最近普及しているカード形状の容器にIC素子を封入したICカードが普及し、特にマイクロプロセッサを封入したPCカードが理想的である。

【0124】 また、データ管理プログラムがデータ管理センタ側のエージェントとしての機能を有しているようにし、ユーザがデータ管理センタに申込みを行う場合に自動的にデータコンテンツの利用状況、転送状況等を報告させるようにすることもできる。

【図面の簡単な説明】

【図1】は、本発明第1実施例のデータ管理システムの構成図である。

【図2】は、本発明第2実施例のデータ管理システム構成図である。

【図3】は、本発明第3実施例のデータ管理システム構成図である。

【図4】は、本発明第4実施例のデータ管理システムの処理フローの前半の部分図である。

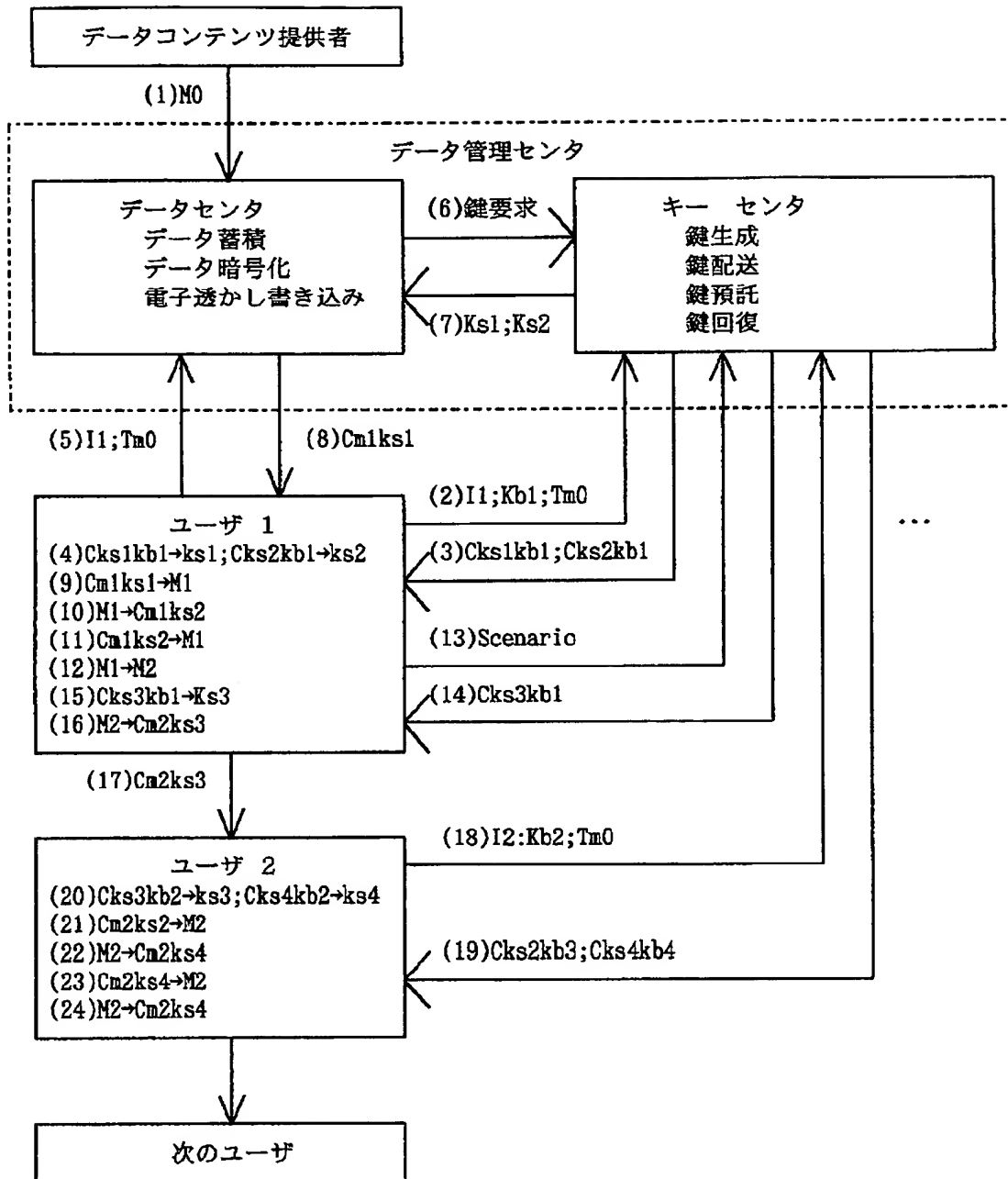
【図5】は、本発明第4実施例のデータ管理システムの処理フローの後半の部分図である。

```

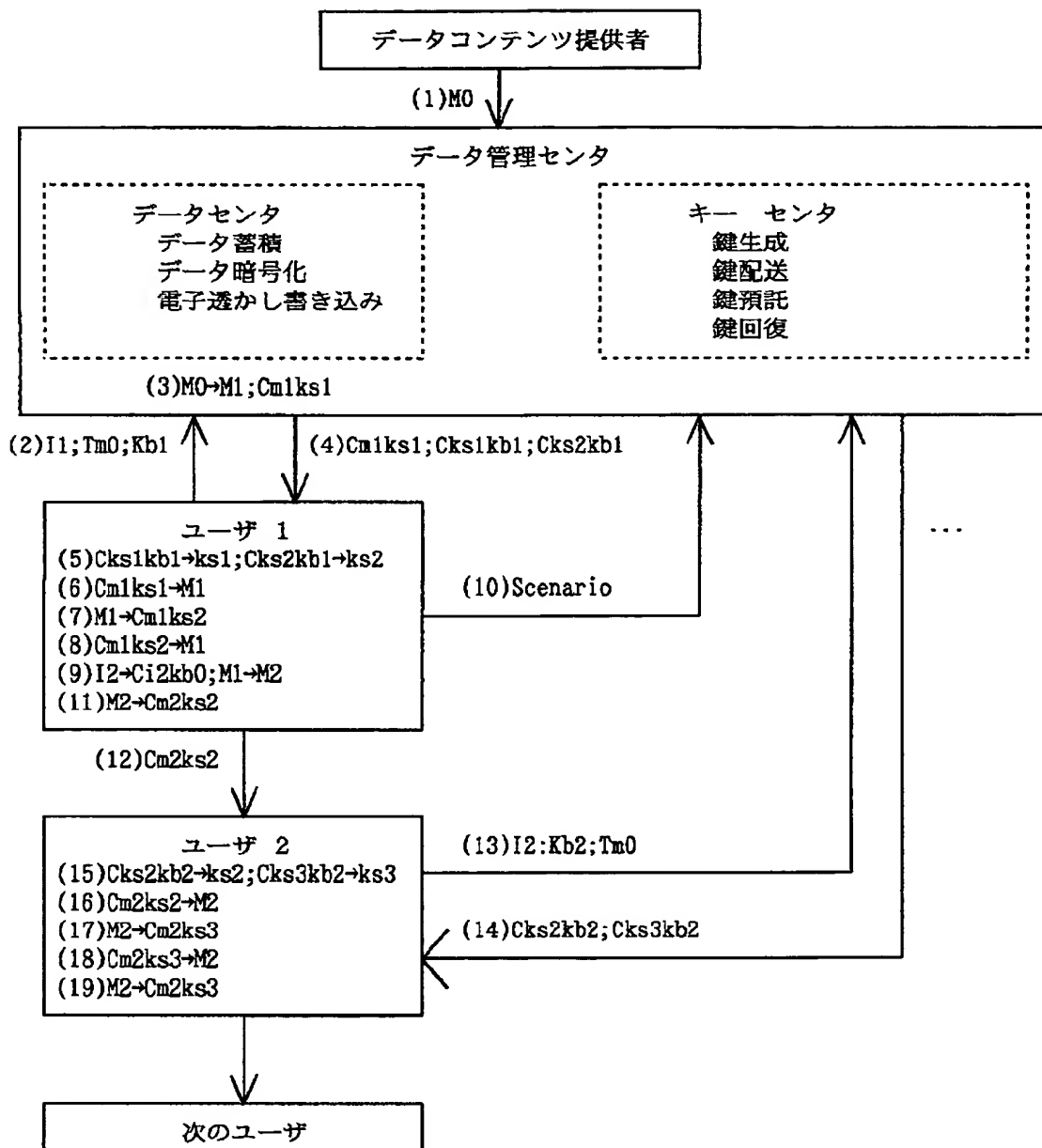
sequenceDiagram
    participant DCP as データコンテンツ提供者
    participant DMC as データ管理センタ
    participant KC as キーセンタ
    participant U1 as ユーザ 1
    participant U2 as ユーザ 2
    participant UN as 次のユーザ

    DCP->>DMC: (1) M0
    DMC->>U1: (5) I1; Tm0
    U1->>KC: (2) I1; Kb1; Tm0
    KC->>DMC: (6) 鍵要求
    DMC->>KC: (7) Ks1; Ks2
    KC->>U1: (3) Cks1kb1; Cks2kb1
    U1->>DMC: (4) Cks1kb1->ks1; Cks2kb1->ks2
    DMC->>KC: (8) Cm1ks1
    KC->>U1: (13) Scenario
    U1->>U2: (15) Cm2ks2
    U2->>KC: (16) I2; Kb2; Tm0
    KC->>U2: (17) Cks2kb2; Cks3kb2
    U2->>DMC: (18) Cks2kb2->ks2; Cks3kb2->ks3
    DMC->>U1: (9) Cm1ks1->M1
    U1->>DMC: (10) M1->Cm1ks2
    DMC->>U1: (11) Cm1ks2->M1
    U1->>DMC: (12) M1->M2
    DMC->>U1: (14) M2->Cm2ks2
    DMC->>U2: (20) M2->Cm2ks3
    U2->>DMC: (21) Cm2ks3->M2
    DMC->>U2: (22) M2->Cm2ks3
    U2->>UN: 
    
```

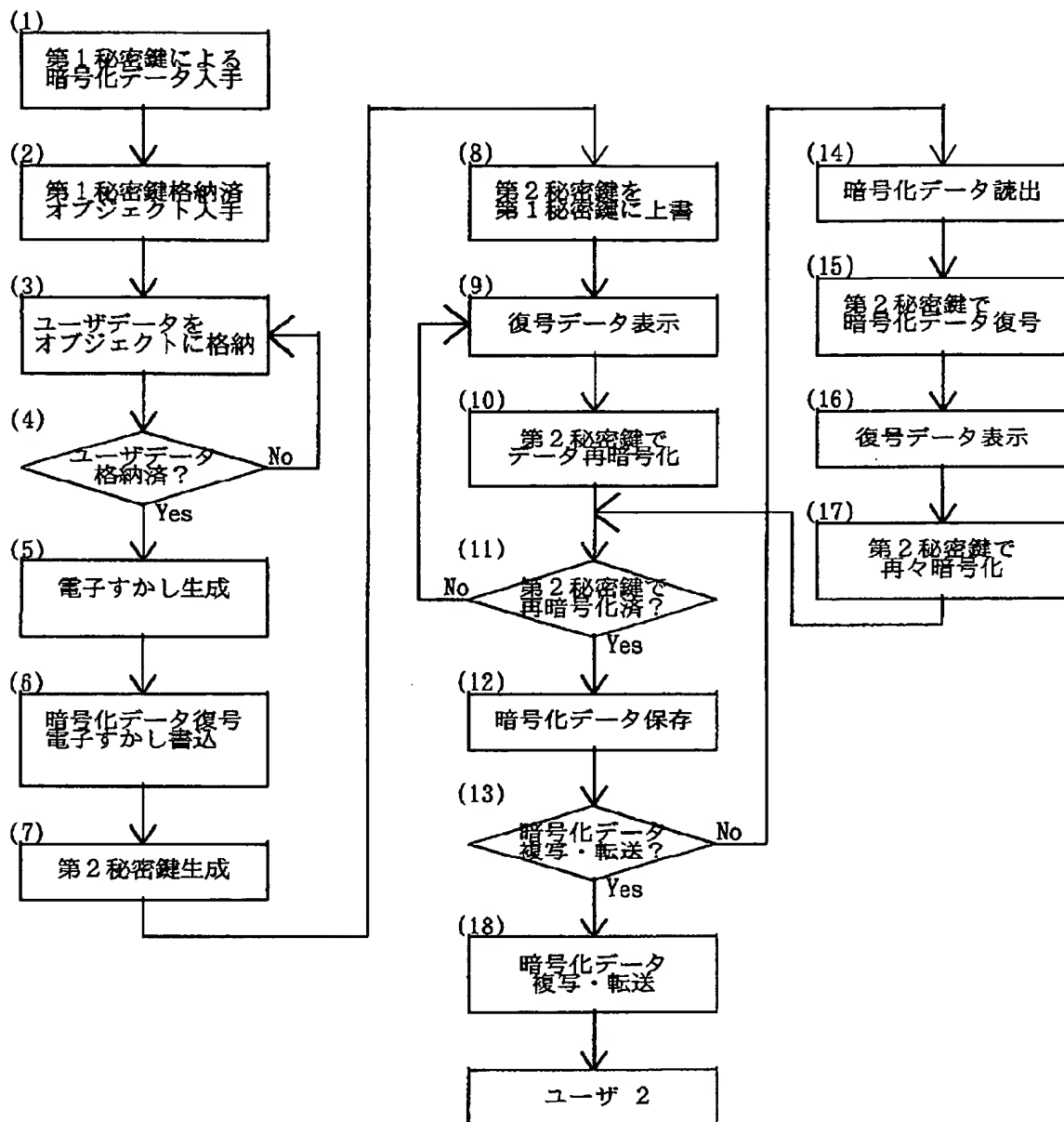
【図2】



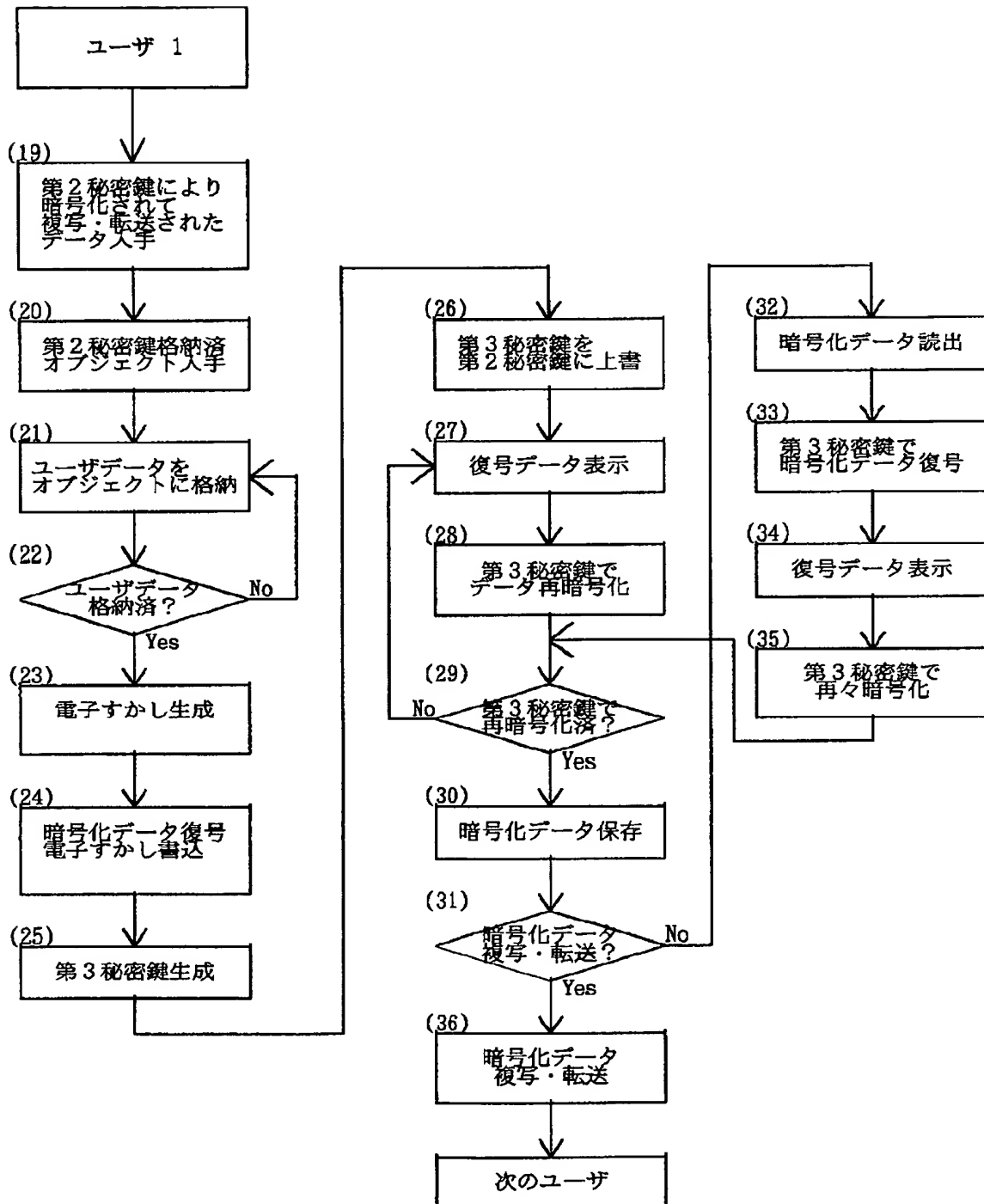
【図3】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

// H 0 4 N 7/167

H 0 4 N 7/167

Z